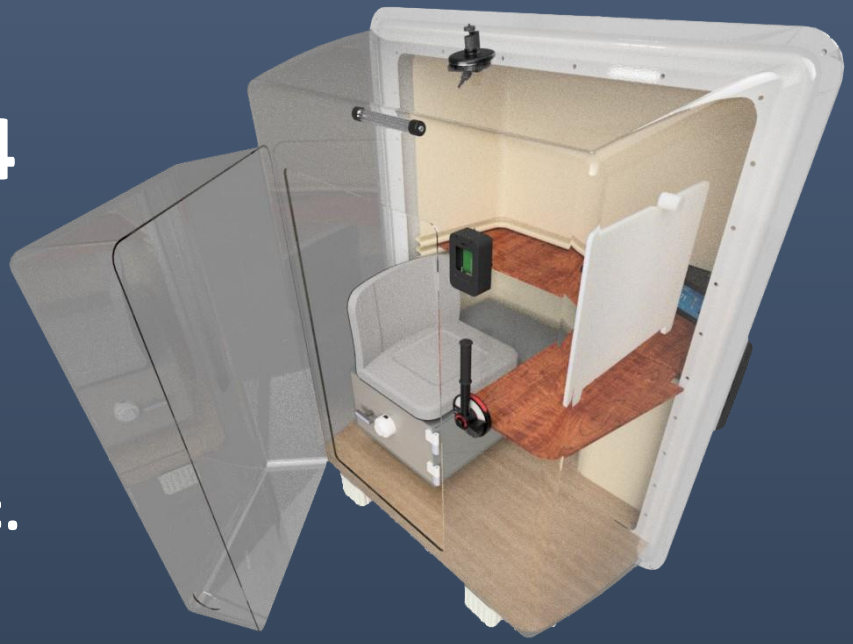
Endpoint Physical Security

Where you need it, When you need it
Expanding success with SIPR to tackle JWICS

DAFITC - 2024

Presented by:

Bob Bauman
President/CEO
Trusted Systems, Inc.



SCIF Reality Check
Mission Creep

- SCIFs secure perimeters & **SPACE** within
- **Mission expanded to a network PORTAL**
- Each access point exposes entire network
- Attention, manpower, funding to Cybersecurity
- Cybersecurity: Inside out, reactive mindset
- Physical Security: Outside in, proactive mindset
- ICD-705 SCIF spec left with shortcomings

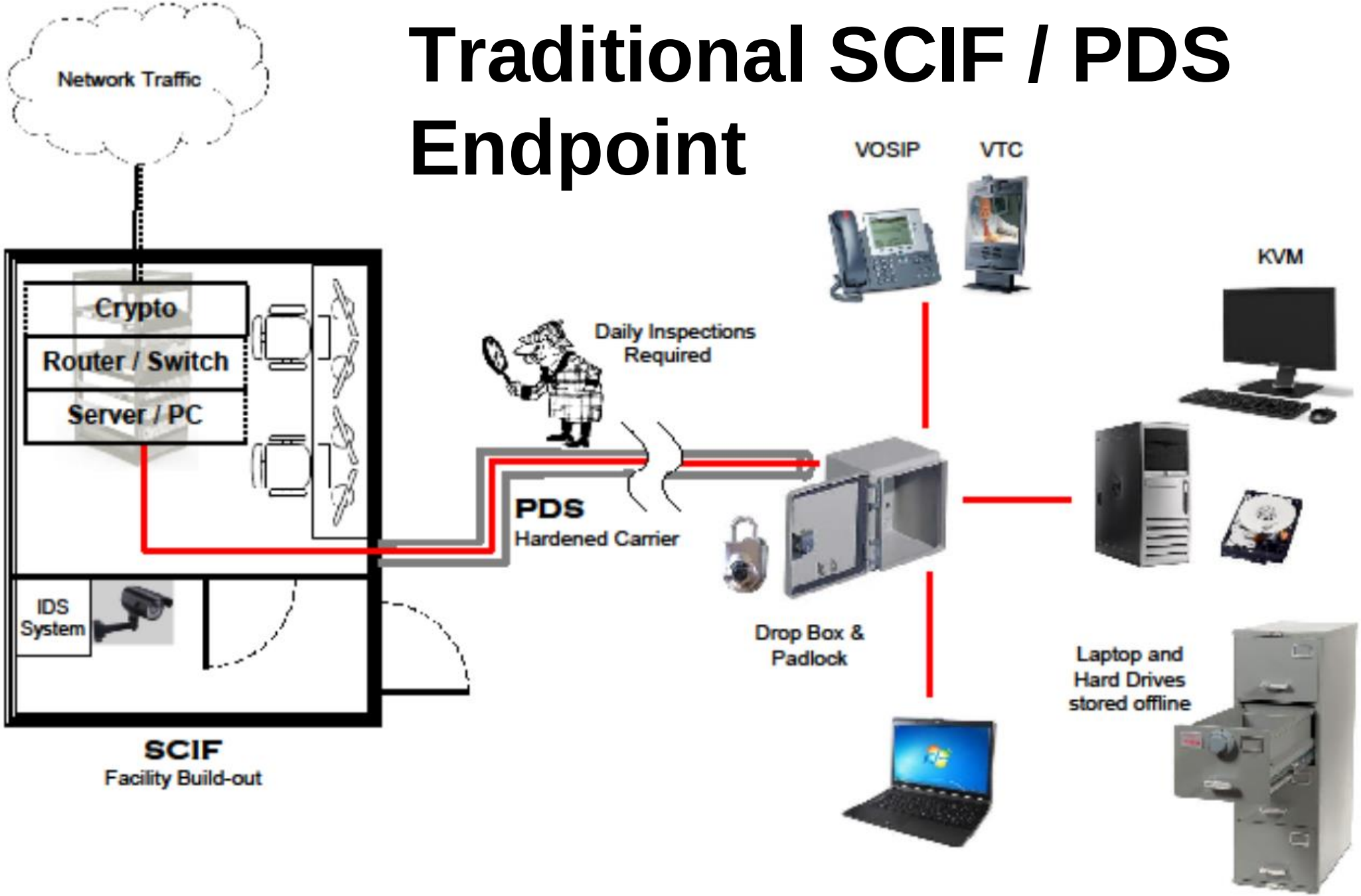
SCIF Shortcomings

- Security tied to the facility, not the network
- Only login at network portal once inside SCIF
  - No isolation of network devices or user interface
  - Alarm systems only detect external activity
- For single seat applications:
  - Too expensive
  - Too time consuming to construct & certify
  - Too bulky, inflexible being fixed plant construction

SCIF Reality Check
It's a People Problem

- Security is ALWAYS a People Problem
  - SCIFs antithesis of Reagan's anthem; "*Trust but Verify*"
  - Opposite of zero trust: all trust + no verify
- Physec policy stops at the **wall**, not the desktop
- Left to discretion of local security officials
- Desktop is most vulnerable to Insider Threats

Traditional SCIF / PDS Endpoint



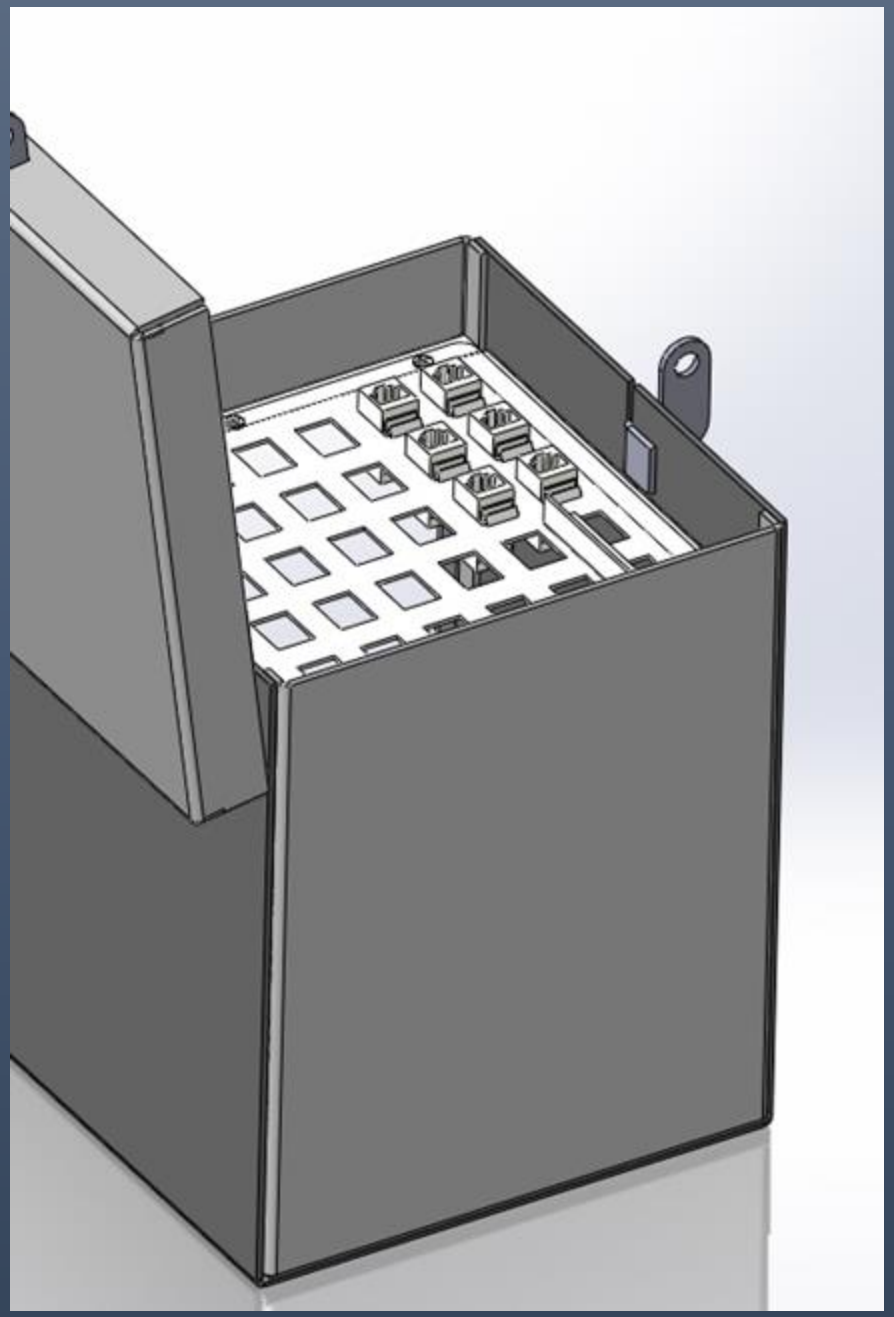
Building Block Approach

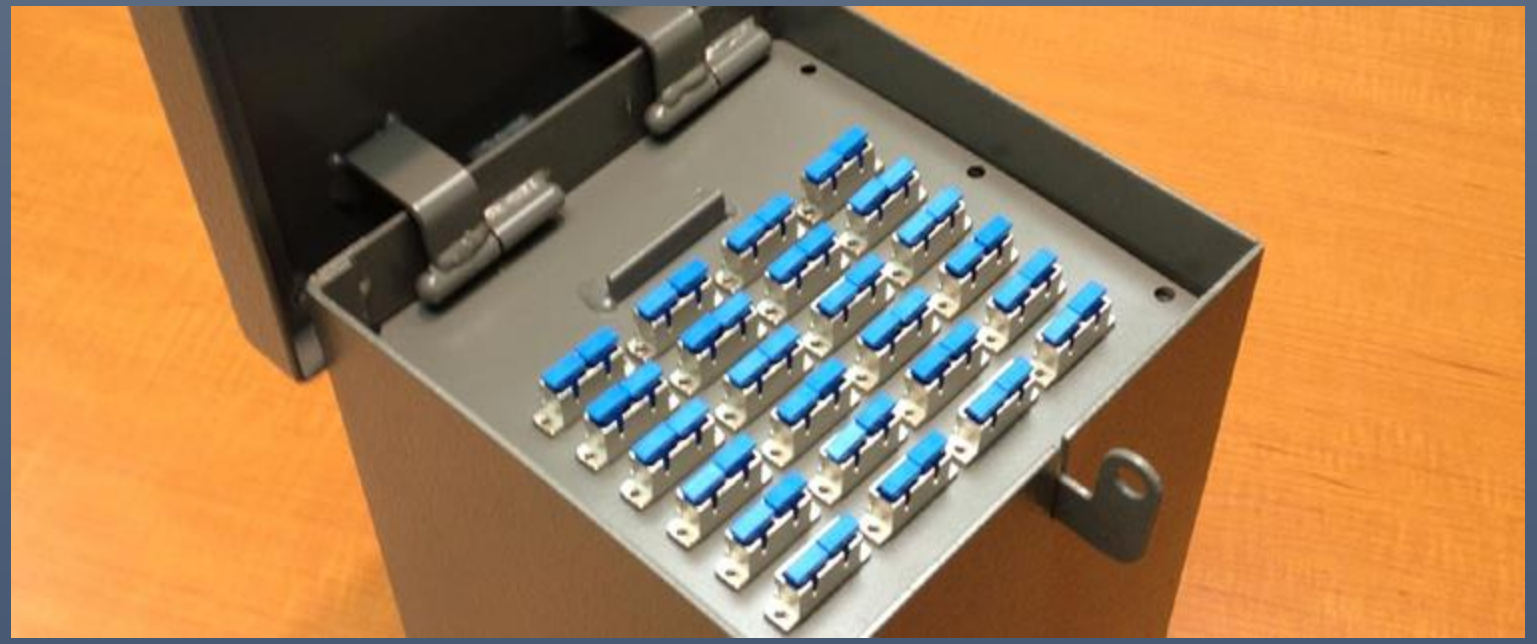
- GSA Class 5 IPS Security Container
  - GSA safe with cooling, rack mounting & cables portals
  - Camouflaging executive matching cabinetry
  - TEMPEST & EMP hardened enclosures
- SIPRNet access controls
  - Desktop user network access
  - Remote monitor and control of network devices
- TS/SCI single seat SCIF equivalent workstation
  - Offsets ICD-705 SCIF shortcomings
  - Tailored for JWICS, SAP and IC networks

IPS Security Container

Executive INCOGNITO SIPRNet Office Suite

TEMPEST and EMP Hardened Enclosures





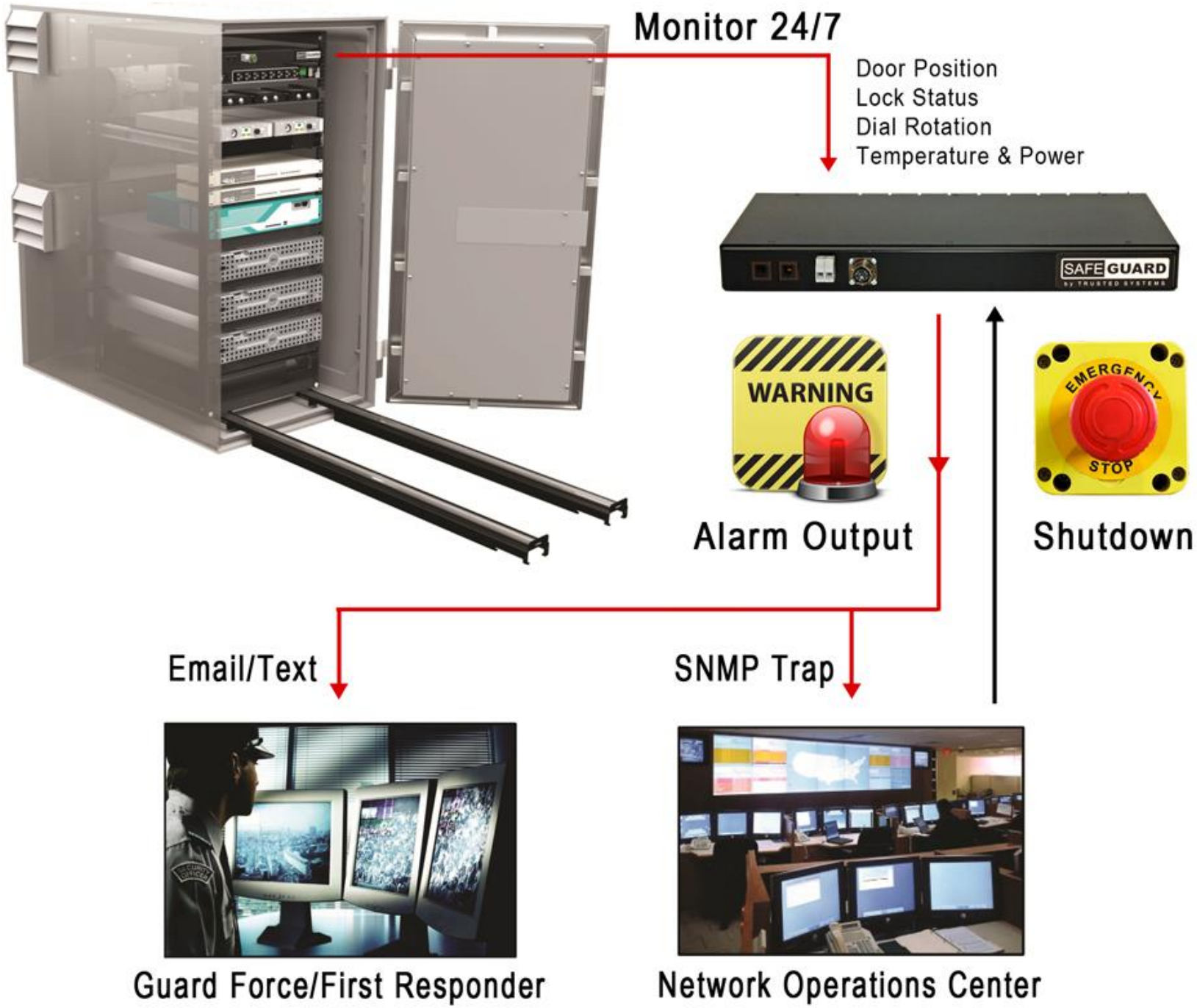
Integrated Drop Box with Patch Panel

SIPRNet Success Story

- DISA STIG only endpoint de facto policy for CCRI compliance
  - Network devices housed in CAA, SCIF, or IPS Container
  - Only authorized network personnel allowed access to devices
- IPS container autonomy augmented with access controls
  - Local desktop access control without need to open IPS Container
  - Continuous remote monitor of IPS lock & door in lieu of alarm system
  - Remote controlled power shutdown upon unauthorized threat alert
- Coincidently, these innovations offset SCIF shortcomings

Two-factor Biometric Access Control System

Network Hardware Remote Monitor & Control System



JWICS Without SCIF Buildout

Solution: build a TEMPEST clamshell to surround the field proven SIPRNet configuration creating:

SoloSCIF™

Single-seat TS/SCI Workstation

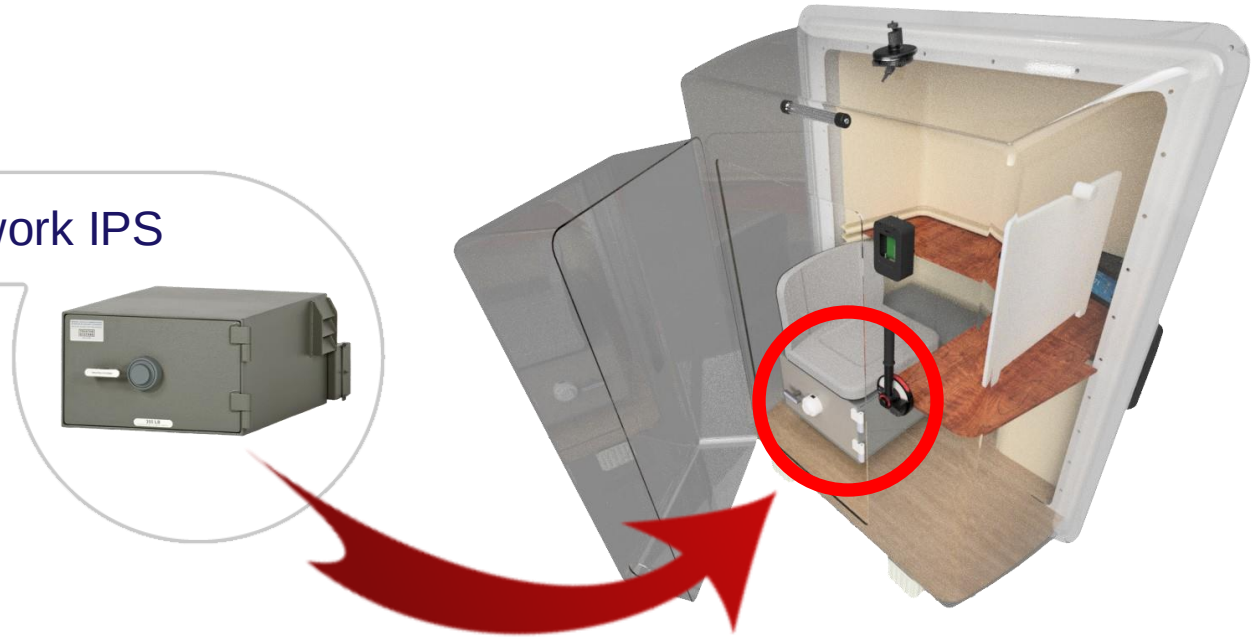
SoloSCIF integrates (3) best-of-breed physical security technologies to create concentric zones of control reinforcing each other for **Defense in Depth**.

Compact • Movable • Cost Effective

Zone 1: Network IPS

IPS: Isolate & secure sensitive network equipment for 24/7 operation.

SafeGuard: Monitor internal environment, lock, door & network status with proactive alarms or shutdown.



Zone 2: Desktop Access Control

IPS: Isolate & secure sensitive network equipment for 24/7 on-line operation.

SafeGuard: Monitor internal environment lock, door & network status with proactive alarms & shutdown.

SIPRGuard: Multi-factor authentication secures operator interface for only authorized users.

Zone 1: Network IPS

Zone 2: Desktop Access Control

Zone 3: Privacy Shielding

IPS: Isolate & secure sensitive network equipment for 24/7 operation.

SafeGuard: Monitor internal environment, lock, door & network status with proactive alarms or shutdown.

SIPRGuard: Multi-factor authentication secures operator interface for only authorized users.

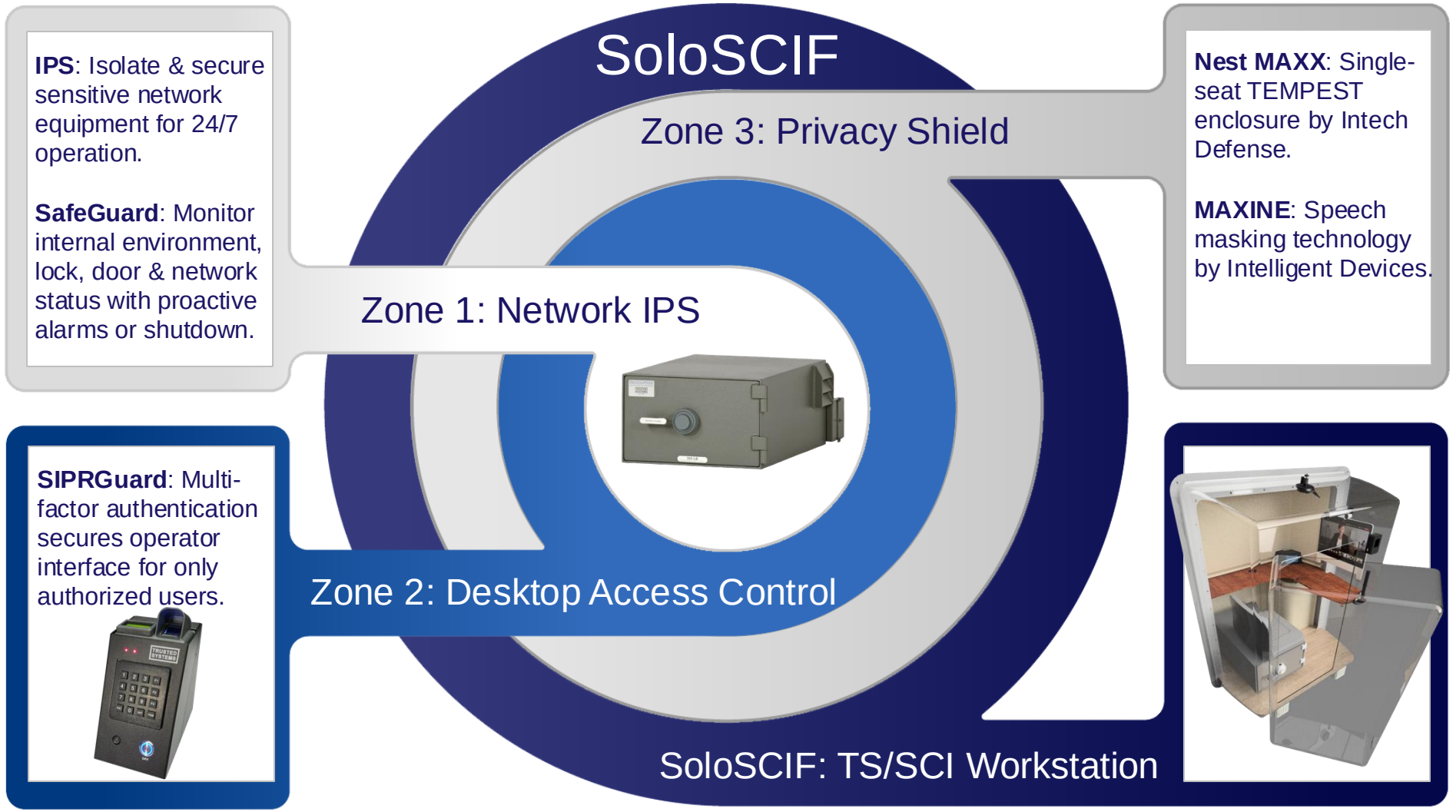
Zone 3: Privacy Shield

Zone 1: Network IPS

Zone 2: Desktop Access Control

Nest MAXX: Single-seat TEMPEST enclosure by Intech Defense.

MAXINE: Speech masking technology by Intelligent Devices.



What's Next?

- A2 SSO/TSCM technical inspections
- Accreditation process with DIA & NSA
- Develop use cases for JWICS expansion
  - HQ offices / teleconferencing
  - Hangers for flight plan downloads
  - Down range regional deployments
  - SAPF remote sites

And Here It Is

Thank you for your time and attention

Bob Bauman
Trusted Systems, Inc.
(703) 624-9236
bob@trustedsys.com
https://trustedsys.com